Claims:

1. A mobile application security system, comprising:

one or more nodes of a peer-to-peer network wherein each node is configured to execute a mobile application;

a central security enforcement node connected to each node of the peer-to-peer network for controlling the security of a mobile application;

the central security enforcement node further comprising means for monitoring the security of the mobile application as it jumps between the nodes wherein data about the mobile application is communicated to the central security enforcement node when the mobile application is communicated from a first node to a second node; and

wherein the security monitoring means further comprises means for detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts.

2. The system of Claim 1, wherein the detecting means further comprises means for storing a copy of the mobile application when the mobile application is created by having the creating node send a copy of the mobile application to the central security enforcement node, means for receiving data about the mobile application when it is received by another node and means for comparing the code of the mobile application received by the other node to the stored copy of the mobile application to determine if changes have been made to the code of the mobile application.

3. The system of Claim 1, wherein the detecting means further comprises means for receiving a checksum of the mobile application when the mobile application is created, means

for receiving the mobile application after it is sent to another node, means for computing the checksum of the received mobile application and means for comparing the checksum of the mobile application after it is received by another node to the stored checksum of the mobile application to determine if changes have been made to the code of the mobile application.

4. A mobile application security system, comprising:

one or more nodes of a peer-to-peer network wherein each node is configured to execute a mobile application;

a central security enforcement node connected to each node of the peer-to-peer network for controlling the security of a mobile application;

the central security enforcement node further comprising means for monitoring the security of the mobile application as it jumps between the nodes wherein data about the mobile application is communicated to the central security enforcement node when the mobile application is communicated from a first node to a second node; and

wherein the security monitoring means further comprises means for preventing a node from transmitting hostile code in a mobile application to another node.

5. The system of Claim 4, wherein the preventing means further comprises means for determining if the node dispatching the mobile application is trusted, means for stripping the code from an initially received mobile application if the host is not trusted, means for saving the code of the mobile application, and means, when requested by another node, for providing the code for the mobile application to the requesting node.

6. A mobile application security system, comprising:

one or more nodes of a peer-to-peer network wherein each node is configured to execute a mobile application;

a central security enforcement node connected to each node of the peer-to-peer network for controlling the security of a mobile application;

the central security enforcement node further comprising means for monitoring the security of the mobile application as it jumps between the nodes wherein data about the mobile application is communicated to the central security enforcement node when the mobile application is communicated from a first node to a second node; and

wherein security monitoring means further comprises means for detecting unwanted changes in the state of the mobile application.

7. The system of Claim 6, wherein the detecting means further comprises means for saving a copy of the state of a mobile application received from a node that received the mobile application, means for receiving data about the same mobile application after a jump to another node and means for comparing the state of the mobile application after the jump to another node with the stored state of the mobile application to ensure that the state of the mobile application has not changed.

8. A mobile application security system, comprising:

one or more nodes of a peer-to-peer network wherein each node is configured to execute a mobile application;

a central security enforcement node connected to each node of the peer-to-peer network for controlling the security of a mobile application;

the central security enforcement node further comprising means for monitoring the security of the mobile application as it jumps between the nodes wherein data about the mobile application is communicated to the central security enforcement node when the mobile application is communicated from a first node to a second node; and

wherein the security monitoring means further comprises means for detecting unwanted changes in the itinerary of the mobile application.

9. The system of Claim 8, wherein the detecting means further comprises means for saving a copy of the itinerary of a mobile application received from the node that received the mobile application, means for receiving the same mobile application after a jump to another node and means for comparing the itinerary of the mobile application after the jump to another node with the stored itinerary of the mobile application to ensure that the itinerary of the mobile application has not changed.

10. The system of Claim 8, wherein the itinerary comprises past historical itinerary data.

11. A mobile application security method, comprising:

receiving data about a mobile application at a central security enforcement node each time the mobile application jumps between a first node and a second node of a peer-to-peer network; and

monitoring the security of the mobile application as it jumps between the nodes, wherein the security monitoring further comprises detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts.

12. The method of Claim 11, wherein the detecting further comprises storing a copy of the mobile application when the mobile application is created, receiving the mobile application after it is received by another node and comparing the code of the mobile application after it is received by another node to the stored copy of the mobile application to determine if changes have been made to the code of the mobile application.

13. A mobile application security method, comprising:

receiving data about a mobile application at a central security enforcement node each time the mobile application jumps between a first node and a second node of a peer-to-peer network; and

monitoring the security of the mobile application as it jumps between the nodes, wherein the security monitoring further comprises preventing a host from transmitting hostile code in a mobile application to another node.

14. The method of Claim 13, wherein the preventing further comprises determining if the node dispatching the mobile application is trusted, stripping the code from a mobile application if the host is not trusted, saving the code of the mobile application, and, when requested by another node, providing the code for the mobile application to the requesting node.

15. A mobile application security method, comprising:

receiving data about a mobile application at a central security enforcement node each time the mobile application jumps between a first node and a second node of a peer-to-peer network; and

monitoring the security of the mobile application as it jumps between the nodes, wherein the security monitoring further comprises detecting unwanted changes in the state of the mobile application.

16. The method of Claim 15, wherein the detecting further comprises saving a copy of the state of a received mobile application, receiving data about the same mobile application after a jump to another node and comparing the state of the mobile application after the jump to another node with the stored state of the mobile application to ensure that the state of the mobile application has not changed.

Sub a1

17. A mobile application security method, comprising:

receiving data about a mobile application at a central security enforcement node each time the mobile application jumps between a first node and a second node of a peer-to-peer network; and

monitoring the security of the mobile application as it jumps between the nodes, wherein the security monitoring further comprises detecting unwanted changes in the itinerary of the mobile application.

18. The method of Claim 17, wherein the detecting further comprises saving a copy of the itinerary of a received mobile application, receiving data about the same mobile application after a jump to another node and comparing the itinerary of the mobile application after the jump to another node with the stored itinerary of the mobile application to ensure that the itinerary of the mobile application has not changed.

19. The method of Claim 17, wherein the itinerary comprises past historical itinerary data.

20. A mobile application security method, comprising:

receiving data about a mobile application at a central security enforcement node each time the mobile application jumps between a first node and a second node of a peer-to-peer network; and

monitoring the security of the mobile application as it jumps between the nodes, wherein the security monitoring further comprises preventing untrusted hosts from initially launching mobile applications